IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

RAYMOND CHAO, individually and on behalf of all others similarly situated,

Plaintiff,

v.

TRUSTEES OF COLUMBIA UNIVERSITY d/b/a COLUMBIA UNIVERSITY,

Defendant.

Case No.:_____

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff, Raymond Chao, ("Plaintiff") brings this Class Action Complaint against Defendant Trustees of Columbia University d/b/a Columbia University ("Columbia" or "Defendant") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to Plaintiff's own actions and to counsels' investigation, and upon information and belief as to all other matters, as follows:

PARTIES, JURISDICTION & VENUE

1. Plaintiff Raymond Chao is a resident and citizen of Brooklyn, New York.

2. Defendant Trustees of Columbia University d/b/a Columbia University is a nonprofit corporation organized under the laws of New York with its principal place of business at West 116 Street and Broadway, New York, NY 10027

3. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C.§1332, because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000.00, exclusive of interest and costs, there are

more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from each Defendant.

4. This Court has personal jurisdiction over Defendant Trustees of Columbia University d/b/a Columbia University because its principal place of business is in New York, and it does a significant amount of business in New York.

5. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant Trustees of Columbia University d/b/a Columbia University has its principal place of business located in this District, and a substantial part of the events giving rise to this action occurred in this District.

STATEMENT OF FACTS

6. This class action arises out of the recent targeted ransomware attack and data breach ("Data Breach") on Defendant's network that resulted in unauthorized access to 460gigabytes of information representing approximately 2.5 million applicants. Data acquired in the breach included 1.8 million social security numbers, financial aid package information, and employee pay stubs.[1] As a result of the Data Breach, Class Members suffered ascertainable losses in the form of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the present risk of imminent harm caused by the compromise of their sensitive personal information.

7. Defendant Columbia University is a self-proclaimed "leader in higher education for more than 250 years." [2]

[1] *See*, https://www.theverge.com/analysis/703232/columbia-hack-admissions-data-mamdani (last visited July 10, 2025).

[2]https://undergrad.admissions.columbia.edu/academics#:~:text=A%20leader%20in%20higher%20education,advancement%20of%20our%20global%20society. (last visited July 10, 2025).

8. Upon information and belief, Defendant collects personal data in connection with its business. This personally identifiable information ("PII") includes the sensitive data which was compromised in the Data Breach alleged herein.

9. Defendant acknowledges the benefits it receives in collecting this information, stating in its "Information Security Charter" that "[s]uch information is an important resource of the University and any person who uses the information collected by the University has a responsibility to maintain and protect this resource."[3]

10. Upon information and belief, Defendant promises to maintain the confidentiality of Plaintiff's and Class Members' Private Information to ensure compliance with federal and state laws and regulations, and not to use or disclose Plaintiff's and Class Members' Private Information for non-essential purposes.

11. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

12. Defendant recognizes these duties, declaring in its "Information Security Charter" that:

a. "Federal and state laws and regulations, as well as industry standards, also impose obligations on the University to protect the confidentiality, integrity and availability of information relating to faculty, staff, students, research subjects and patients;"

b. "In addition, terms of certain contracts and University policy require appropriate safeguarding of information;" and

[3] https://universitypolicies.columbia.edu/content/information-security-charter (last visited July 10, 2024).

c. "The mission of the Information Security Program is to protect the confidentiality, integrity and availability of University Data. Confidentiality means that information is only accessible to authorized users. Integrity means safeguarding the accuracy and completeness of University Data and processing methods."[4]

13. Additionally, Defendant's policy for "Handling Personally Identifying Information-PII" states:

a. "Stolen PII is frequently used to commit identity theft and fraud, and should be guarded carefully. Hackers and malware will search a compromised computer for SSN's they can find;"

b. "As a matter of good practice, you should never keep any unprotected PII on your workstation. For Columbia employees and equipment, any PII should be protected with strong encryption or removed;" and

c. "The capture, storage and retention of confidential and sensitive information by CUIT employees is permissible only if it is a University business requirement and complies with Columbia University's Social Security Number Usage Policy, Data Classification Policy and University Requirements for Endpoints Containing Sensitive Data Policy."[5]

14. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class Members would not have entrusted Defendant with their Private Information had they known that Defendant would fail to implement industry standard protections for that sensitive information.

[4] *Id.*
[5] https://www.cuit.columbia.edu/handling-pii (last visited July 10, 2024).

15. Plaintiff and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

The Data Breach

16. On or about June 24, 2025, Defendant announced that it was investigating "widespread system outages" affecting its online platforms.[6]

17. The "widespread system outages" were first reported by the Columbia University Information Technology (CUIT) department at around 7:30 a.m. in an email blast sent out to all students and faculty.[7]

18. Several of Defendant's most important online tools were impacted.[8] These include:

a. The UNI Login System: This is what everyone at Columbia uses to sign into websites, email, and apps. Without it, students and staff were locked out of almost everything.

b. LionMail: This is Columbia's email system, which runs on Google's Gmail. Students and teachers couldn't send or receive emails, making it hard to communicate.

c. CourseWorks: This is the online classroom where students get assignments, submit homework, and talk to their professors. Without it, many classes couldn't run normally.

[6] https://cybernews.com/news/columbia-university-suspected-cyberattack-systemwide-outage/ (last visited July 10, 2025).
[7] *Id.*
[8] https://newsinterpretation.com/columbia-university-hit-by-widespread-digital-outage/

19. Worryingly, this incident is only part and parcel of Defendant's pattern of negligent data security. In May 2024, The Cyber Express, a cybersecurity news site, reported that a cybercriminal group claimed credit for a cyberattack on Columbia.[9]

20. Additionally, in 2007, Columbia exposed 2,600 Social Security numbers belonging to its undergraduate students and alumni.[10] As a result of this security breach, Defendant sent letters to affected students and alumni, encouraging them to monitor their credit to guard against identity theft.[11] These previous incidents further evidence Defendant's lack of adequate cybersecurity measures.

21. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's PII was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the PII from those risks left the data in a dangerous condition.

22. The Data Breach was a direct result of Defendant's failure to implement an information security program designed to: (a) to ensure the security and confidentiality of information; (b) to protect against anticipated threats or hazards to the security or integrity of that information; and (c) to protect against unauthorized access to that information that could result in substantial harm or inconvenience to any individual.

23. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

[9] https://thecyberexpress.com/cyberattack-on-columbia-university/#google_vignette
[10] https://spectatorarchive.library.columbia.edu/?a=d&d=cs20070418-01.2.5&srpos=1&e=-------en-20--1--txt-txIN---------
[11] *Id.*

24. Because of Defendant's Data Breach, the sensitive PII of Plaintiff and Class members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class members.

25. Defendant has not provided any assurances that: all data acquired in the Data Breach, or copies thereof, have been recovered or destroyed; or, that Defendant has modified its data protection policies, procedures, and practices sufficient to avoid future, similar, data breaches.

26. Defendant's failure to adequately secure the PII in its custody, has created a separate, particularized, and concrete harm to the Plaintiff.

27. More specifically, the Plaintiff's exposure to the substantial risk of future exploitation caused or will cause them to: (i) spend money on mitigation measures like credit monitoring services and/or dark web searches; (ii) lose time and effort spent responding to the Data Breach; and/or (iii) experience emotional distress associated with reviewing accounts for fraud, changing usernames and passwords or closing accounts to prevent fraud, and general anxiety over the consequences of the Data Breach. The harm Plaintiff's suffered can be redressed by a favorable decision in this matter.

Data Breaches Are Avoidable

28. Upon information and belief, the Data Breach was a direct result of Defendant's failure to: (i) identify risks and potential effects of collecting, maintaining, and sharing personal information; (ii) adhere to its published privacy practices; (iii) implement reasonable data protection measures for the collection, use, disclosure, and storage of personal information; and/or (iv) ensure its third-party vendors were required to implement reasonable data protection measures consistent with Defendant's data protection obligations.

29. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's PII was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the PII from those risks left the data in a dangerous condition.

30. Upon information and belief, the Data Breach occurred as the result of a ransomware attack. In a ransomware attack, the attackers use software to encrypt data on a compromised network, rendering it unusable and then demand payment to restore control over the network.[12] Ransomware groups frequently implement a double extortion tactic, "where the cybercriminal **posts portions of the data** to increase their leverage and force the victim to pay the ransom, and then sells the stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[13]

31. To detect and prevent cyber-attacks, Defendant could and should have implemented the following measures:

Reasonable Safeguards

a. Regularly patch critical vulnerabilities in operating systems, software, and firmware on devices. Consider using a centralized patch management system.
b. Check expert websites (such as www.us-cert.gov) and your software vendors' websites regularly for alerts about new vulnerabilities and implement policies for installing vendor-approved patches to correct problems.
c. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks. Depending on your circumstances, appropriate assessments may range from having a knowledgeable employee run off-the-shelf security software to having an independent professional conduct a full-scale security audit.
d. Scan computers on your network to identify and profile the operating system and open network services. If you find services that you don't need, disable them to prevent hacks or other potential security problems.

[12] *Ransomware FAQs*, https://www.cisa.gov/stopransomware/ransomware-faqs (last visited July 10, 2024).
[13] *Ransomware: The Data Exfiltration and Double Extortion Trends*, https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends (last visited July 10, 2024).

e. Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

f. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email.

g. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

h. Configure firewalls to block access to known malicious IP addresses.

i. Set anti-virus and anti-malware programs to conduct regular scans automatically.

j. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

k. Configure access controls—including file, directory, and network share permissions— with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

l. Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

m. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

n. Consider disabling Remote Desktop protocol (RDP) if it is not being used.

o. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

p. Execute operating system environments or specific programs in a virtualized environment.

q. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

r. Conduct an annual penetration test and vulnerability assessment.

s. Secure your backups.[14]

t. Identify the computers or servers where sensitive personal information is stored.

u. Identify all connections to the computers where you store sensitive information. These may include the internet, electronic cash registers, computers at your branch offices, computers used by service providers to support your network, digital copiers, and wireless devices like smartphones, tablets, or inventory scanners.

[14] *How to Protect Your Networks from Ransomware*, at p.3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited July 10, 2024).

v. Don't store sensitive consumer data on any computer with an internet connection unless it's essential for conducting your business.

w. Encrypt sensitive information that you send to third parties over public networks (like the internet) and encrypt sensitive information that is stored on your computer network, laptops, or portable storage devices used by your employees. Consider also encrypting email transmissions within your business.

x. Regularly run up-to-date anti-malware programs on individual computers and on servers on your network.

y. Restrict employees' ability to download unauthorized software. Software downloaded to devices that connect to your network (computers, smartphones, and tablets) could be used to distribute malware.

z. To detect network breaches when they occur, consider using an intrusion detection system.

aa. Create a "culture of security" by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities.

bb. Tell employees about your company policies regarding keeping information secure and confidential. Post reminders in areas where sensitive information is used or stored, as well as where employees congregate.

cc. Teach employees about the dangers of spear phishing—emails containing information that makes the emails look legitimate. These emails may appear to come from someone within your company, generally someone in a position of authority. Make it office policy to independently verify any emails requesting sensitive information.

dd. Before you outsource any of your business functions investigate the company's data security practices and compare their standards to yours.[15]

32. Given that Defendant collected, used, and stored PII, Defendant could and should have identified the risks and potential effects of collecting, maintaining, and sharing personal information.

33. Without identifying the potential risks to the personal data in Defendant's possession, Defendant could not identify and implement the necessary measures to detect and prevent cyberattacks. The occurrence of the Data Breach indicates that Defendant failed to

[15] *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited July 10, 2024).

adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of Plaintiff's and the Class Members' PII.

34. Defendant knew and understood unencrypted PII is valuable and highly sought after by cybercriminals seeking to illegally monetize that data. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if a data breach occurred, including the significant cost that would be imposed on Plaintiff and the Class Members as a result.

Plaintiff and Class Members Sustained Damages in the Data Breach

35. The invasion of the Plaintiff's and Class Members' privacy suffered in this Data Breach constitutes an actual, particularized, redressable injury traceable to the Defendant's conduct. As a consequence of the Data Breach, Plaintiff and Class Members sustained monetary damages that exceed the sum or value of $5,000,000.00.

36. Additionally, Plaintiff and Class Members face a substantial risk of future identity theft, fraud, or other exploitation where their names and social security numbers were targeted by a sophisticated hacker known for stealing and reselling sensitive data on the dark web. The substantial risk of future identity theft and fraud created by the Data Breach constitutes a redressable injury traceable to the Defendant's conduct.

37. Upon information and belief, a criminal can easily link data acquired in the Data Breach with information available from other sources to commit a variety of fraud related crimes. An example of criminals piecing together bits and pieces of data is the development of "Fullz" packages.[16] With "Fullz" packages, cyber-criminals can combine multiple sources of PII to apply for credit cards, loans, assume identities, or take over accounts.

[16] "Fullz" is term used by cybercriminals to describe "a package of all the personal and financial records that thieves would need to fraudulently open up new lines of credit in a person's name." A Fullz package

38. Given the type of targeted attack in this case, the sophistication of the criminal claiming responsibility for the Data Breach, the type of PII involved in the Data Breach, the hacker's behavior in prior data breaches, the ability of criminals to link data acquired in the Data Breach with information available from other sources, and the fact that the stolen information has been placed, or will be placed, on the dark web, it is reasonable for Plaintiff and the Class Members to assume that their PII was obtained by, or released to, criminals intending to utilize the PII for future identity theft-related crimes or exploitation attempts.

39. The substantial risk of future identity theft, fraud, or other exploitation that Plaintiff and Class Members face is sufficiently concrete, particularized, and imminent that it necessitates the present expenditure of funds to mitigate the risk. Consequently, Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to understand and mitigate the effects of the Data Breach.

40. For example, the Federal Trade Commission has recommended steps that data breach victims take to protect themselves and their children after a data breach, including: (i) contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity); (ii) regularly obtaining and reviewing their credit reports; (iii) removing fraudulent charges from their accounts; (iv) closing new accounts opened in their name; (v) placing a credit freeze on their credit; (vi) replacing government-issued identification; (vii) reporting misused Social Security numbers; (viii) contacting utilities to ensure

typically includes the victim's name, address, credit card information, social security number, date of birth, bank name, routing number, bank account numbers and more. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm (last visited July 10, 2024).

no one obtained cable, electric, water, or other similar services in their name; and (ix) correcting their credit reports.[17]

41. As a consequence of the Data Breach, Plaintiff and Class Members sustained or will incur monetary damages to mitigate the effects of an imminent risk of future injury. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year. The cost of dark web scanning and monitoring services can cost around $180 per year.

42. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and illegitimate markets, has been damaged and diminished by its unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

43. Personal information is of great value, in 2019, the data brokering industry was worth roughly $200 billion.[18] Data such as name, address, phone number, and credit history has been sold at prices ranging from $40 to $200 per record.[19] Sensitive PII can sell for as much as $363 per record.[20]

44. Furthermore, Defendant's poor data security practices deprived Plaintiff and Class Members of the benefit of their bargain. By transacting business with Plaintiff and Class Members,

---

[17] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 10, 2024).

[18] *Column: Shadowy data brokers make the most of their invisibility cloak*, https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited July 10, 2024).

[19] *In the Dark*, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited July 10, 2024).

[20] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

collecting their PII, using their PII for profit or to improve the ability to make profits, and then permitting the unauthorized disclosure of the PII, Plaintiff and Class Members were deprived of the benefit of their bargain.

45. When agreeing to pay Defendant for services, consumers understood and expected that they were, in part, paying for the protection of their personal data, when in fact, Defendant did not invest the funds into implementing reasonable data security practices. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff's Injuries

46. Plaintiff Raymond Chao is a former student of Defendant—having graduated in 2021.

47. Thus, Defendant obtained and maintained Plaintiff's PII

48. As a result, Plaintiff was injured by Defendant's Data Breach.

49. As a condition of receiving educational services, Plaintiff provided Defendant with his PII. Defendant used that PII to facilitate its provision of educational services and to collect payment.

50. Plaintiff provided his PII to Defendant and trusted the university would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

51. Plaintiff reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of PII.

52. On information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

53. Through its Data Breach, Defendant compromised Plaintiff's PII.

54. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft, contacting counsel, and researching the Data Breach.

55. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach.

56. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

57. Plaintiff suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

58. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

59. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's PII right in the hands of criminals.

60. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

61. Today, Plaintiff has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

62. Through this Complaint, Plaintiff seeks redress individually, and on behalf of all similarly situated individuals, for the damages that resulted from the Data Breach.

CLASS ALLEGATIONS

63. Plaintiff brings this nationwide class action individually, and on behalf of all similarly situated individuals, pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

64. The Class that Plaintiff seeks to represent is defined as follows:

> **Nationwide Class**: All individuals whose PII was accessed and/or acquired by an unauthorized party in the Data Breach (the "Class").

65. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

66. Plaintiff reserves the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

67. Numerosity: The members of the Classes are so numerous that joinder of all members is impracticable, if not completely impossible. While the exact number of Class Members is unknown to Plaintiff at this time and such number is exclusively in the possession of Defendant, upon information and belief, millions of individuals were impacted by the Data Breach.

68. Common questions of law and fact exist as to all members of the Classes and predominate over any questions affecting solely individual members of the Classes. The questions of law and fact common to the Classes that predominate over questions which may affect individual Class Members, includes the following:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their PII;

f. Whether Defendant breached its duty to Class Members to safeguard their PII;

g. Whether computer hackers obtained Class Members' PII in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent; and;

k. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

69. Typicality: Plaintiff's claims are typical of those of the other members of the Classes because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Classes.

70. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect

to the Classes as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenges of these policies hinges on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiff.

71. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

72. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

73. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since Defendant would be able to exploit and overwhelm the limited resources of each

individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

74. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

75. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

76. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Classes, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

77. Further, Defendant has acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

78. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the Plaintiff and the Classes of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, sharing, storing, and safeguarding their PII;

c. Whether Defendant's security measures to protect its network were reasonable in light of industry best practices;

d. Whether Defendant's (or their vendors') failure to institute adequate data protection measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII;

f. Whether Defendant made false representations about their data privacy practices and commitment to the security and confidentiality of customer information; and

g. Whether adherence to industry standards and best practices for protecting personal information would have reasonably prevented the Data Breach.

CAUSES OF ACTION
(*On behalf of Plaintiff and the Classes*)

COUNT 1

NEGLIGENCE/WANTONNESS

79. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

80. Defendant obtains sensitive PII from its applicants and employees, including Plaintiff and Class Members, in the ordinary course of business.

81. Plaintiff and Class Members were required to entrust Defendant with their PII with the understanding that Defendant would adequately safeguard their information.

82. Defendant had full knowledge of the types of PII it collected and the types of harm that Plaintiff and Class Members would suffer if that data was accessed and exfiltrated by an unauthorized third-party.

83. By collecting, storing, sharing, and using the Plaintiff's and Class Members' PII, Defendant assumed a duty to use reasonable means to safeguard the personal data it obtained.

Defendant's duty included a responsibility to ensure it: (i) implemented reasonable administrative, technical, and physical measures to detect and prevent unauthorized intrusions into its information technology environment; (ii) contractually obligated its vendors to adhere to the requirements of Defendant's privacy policy; (iii) complied with applicable statutes and data protection obligations; (iv) conducted regular privacy assessments and security audits of Defendant's and/or its vendors' data processing activities; (v) regularly audited for compliance with contractual and other applicable data protection obligations; and, (vi) provided timely notice to individuals impacted by a data breach event.

84. Defendant also had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits unfair or deceptive trade practices that affect commerce, such as failing to adhere to a company's own published privacy policies.

85. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII that Defendant was no longer required to retain.

86. Defendant had a duty to notify Plaintiff and the Classes of the Data Breach promptly and adequately. Such notice was necessary to allow Plaintiff and the Classes to take steps to prevent, mitigate, and repair any fraudulent usage of their PII.

87. Defendant violated Section 5 of the FTC Act by failing to adhere to its own privacy policy regarding the confidentiality, integrity and availability of Plaintiff and Class Members information. Defendant further violated Section 5 of the FTC Act, and other state consumer protection statutes by failing to implement an information security plan or use reasonable security measures to protect PII. Defendant's violations constitute negligence and/or wantonness.

88. Defendant's failure to adhere to its data privacy and security obligations was a reckless disregard for the Plaintiff's and Class Members' privacy rights. Defendant knew, or should have known, that its failure to take reasonable precautions might result in injury to Plaintiff and Class Members. The negligent and wanton acts or omissions committed by Defendant includes, but is not limited to, the following:

a. Failing to designate a qualified individual to implement and supervise its information security program.
b. Failing to conduct an assessment to determine foreseeable risks and threats – internal and external – to the confidentiality, integrity and availability of personal information.
c. Failing to design and implement safeguards to control the risks identified through the risk assessment.
d. Failing to encrypt personally identifying information in transit and at rest.
e. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII.
f. Failing to adequately monitor the security of its networks and systems.
g. Allowing unauthorized access to PII.
h. Failing to detect in a timely manner that PII had been compromised.
i. Failing to remove former students' PII it was no longer required to retain.
j. Failing to timely and adequately notify Plaintiff and Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

89. Plaintiff and Class Members are within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm the statue was intended to guard against.

90. The injuries resulting to Plaintiff and the Classes because of Defendant's failure to use adequate security measures was reasonably foreseeable.

91. Plaintiff and the Classes were the foreseeable victims of a data breach. Defendant knew or should have known of the inherent risks in collecting and storing PII, the critical

importance of protecting that PII, and the necessity of updating, patching, or fixing critical vulnerabilities in its network.

92. Plaintiff and the Classes had no ability to protect the PII in Defendant's possession. Defendant was in the best position to protect against the harms suffered by Plaintiff and the Classes as a result of the Data Breach.

93. But for Defendant's breach of duties owed to Plaintiff and the Classes, their PII would not have been compromised. There is a close causal connection between Defendant's failure to implement reasonable security measures to protect the PII of Plaintiff and the Classes and the harm, or risk of imminent harm, suffered by Plaintiff and the Classes.

94. As a result of the Data Breach, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

95. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

96. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to: (i) strengthen its data protection procedures; (ii) patch all critical vulnerabilities; and (iii) to provide adequate monitoring and protection to all affected by the Data Breach.

COUNT 2

BREACH OF IMPLIED CONTRACT

97. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

98. Defendant obtains sensitive PII from their applicants and employees, including Plaintiff and Class Members, in the ordinary course of providing services.

99. In so doing, Plaintiff and Class Members entered implied contracts with Defendant by which Defendant agreed to use reasonable technical, administrative, and physical safeguards to protect against unauthorized access to, use of, or disclosure of the personal information it collects and stores.

100. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of an expressed or implied promise to implement reasonable data protection measures.

101. Plaintiff and Class Members fully and adequately performed their obligations under the implied contract with Defendant.

102. Defendant breached the implied contract with Plaintiff and Class Members which arose from the course of conduct between the parties, as well as disclosures on the Defendant's web site, privacy notice, and in other documents, all of which created a reasonable expectation that the personal information Defendant collected would be adequately protected and that the Defendant would take such actions as were necessary to prevent unauthorized access to, use of, or disclosure of such information.

103. As a direct and proximate result of the Defendant's breach of an implied contract, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of

benefit of the bargain; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

104. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to: (i) strengthen its data protection procedures; (ii) patch all critical vulnerabilities; and (iii) to provide adequate monitoring/protection to all affected by the Data Breach.

COUNT 3

INVASION OF PRIVACY

105. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

106. Plaintiff and Class Members had a legitimate expectation of privacy in their sensitive information such as social security numbers. Plaintiff and Class Members were entitled to the protection of this information from disclosure to unauthorized third parties.

107. Defendant owed a duty to Plaintiff and Class Members to keep their PII confidential.

108. Defendant permitted the public disclosure of Plaintiff's and Class Members' PII to unauthorized third parties.

109. The PII that was disclosed without the Plaintiff's and Class Members' authorization was highly sensitive, private, and confidential. The public disclosure of the type of PII at issue here would be highly offensive to a reasonable person of ordinary sensibilities.

110. Defendant permitted its information technology environment to remain vulnerable to foreseeable threats, which created an atmosphere for the Data Breach to occur.

Despite knowledge of the substantial risk of harm created by these conditions, Defendant intentionally disregarded the risk, thus permitting the Data Breach to occur.

111. By permitting the unauthorized disclosure, Defendant acted with reckless disregard for the Plaintiff's and Class Members' privacy, and with knowledge that such disclosure would be highly offensive to a reasonable person. Furthermore, the disclosure of the PII at issue was not newsworthy or of any service to the public interest.

112. Defendant was aware of the potential of a data breach and failed to adequately safeguard its systems and/or implement appropriate policies and procedures to prevent the unauthorized disclosure of Plaintiff's and Class Members' data.

113. Defendant acted with such reckless disregard as to the safety of Plaintiff's and Class Members' PII to rise to the level of intentionally allowing the intrusion upon the seclusion, private affairs, or concerns of Plaintiff and Class Members.

114. Plaintiff and Class Members have been damaged by the invasion of their privacy in an amount to be determined at trial.

COUNT 4

UNJUST ENRICHMENT

115. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

116. Plaintiff brings this Count in the alternative to the breach of implied contract count above.

117. By obtaining their PII, Plaintiff and Class Members conferred a monetary benefit on Defendant. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit.

118. By collecting the PII, Defendant was obligated to safeguard and protect such information, to keep such information confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been compromised or stolen.

119. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, it would be unjust for Defendant to retain any of the benefits that Plaintiff and Class Members conferred upon Defendant without paying value in return.

120. As a direct and proximate result of the Defendant's conduct, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

121. Plaintiff and Class Members are entitled to restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct.

COUNT 5

VIOLATION OF NEW YORK DECEPTIVE TRADE PRACTICES ACT

("GBL") New York Gen. Bus. Law § 349

122. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

123. Under the New York Gen. Bus. Law § 349, "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful."

124. Notably, Defendant's deceptive acts and/or practices were directed at consumers. After all, via its policies, Defendant represented to consumers that they would, inter alia, use reasonably adequate data security.

125. And these deceptive acts—including the quotations provided supra—were materially misleading insofar as they induced consumers to rely on such statements and disclose their PII.

126. Section § 349 applies to Defendant because there is a sufficient nexus between Defendant's conduct and New York. After all, Columbia University is incorporated in New York and its corporate headquarters is in New York, New York.

127. And, upon information and belief, the misleading acts and/or practices alleged herein—including the manifestations in Defendant's data security policies—were written, approved, and/or otherwise authorized by Defendant within the state of New York.

128. In particular, Defendant violated Section § 349 by, inter alia:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' PII, which was a direct and proximate cause of the Data Breach.

b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following

previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach.

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, et seq., which was a direct and proximate cause of the Data Breach.

d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII; and

e. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, et seq.

129. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of their PII.

130. Defendant intended to mislead Plaintiff and Class members and induce them to rely on its omissions.

131. Had Defendant disclosed to Plaintiff and Class members that its data systems were not secure—and thus vulnerable to attack, Defendant would have been unable to continue in business, and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant accepted the PII that Plaintiff and Class members entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Class members acted reasonably in relying on Defendant's omissions, the truth of which they

could not have discovered through reasonable investigation.

132. Defendant acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiff's and Class members' rights.

133. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

134. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

135. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Classes alleged herein, respectfully requests that the Court enter judgment as follows:

A. For an Order certifying this action as a Class action and appointing Plaintiff and her counsel to represent the Class.

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members.

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Breach.

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct.

E. Ordering Defendant to pay for lifetime credit monitoring services for Plaintiff and the Class.

F. For an award of actual damages, compensatory damages, statutory damages and statutory penalties, in an amount to be determined, as allowable by law.

G. For an award of punitive damages, as allowable by law.

H. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded and,

J. All such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of all claims in this Complaint and of all issues in this action so triable as of right.

Dated: Friday, July 11, 2025.

/s/ Thomas J. McKenna
Thomas J. McKenna
Gainey McKenna & Egleston
260 Madison Avenue, 22nd Floor
New York, New York 10016
Telephone: (212) 983-1300
Facsimile: (212) 983-0383
Email: tjmckenna@gme-law.com
Website: www.gme-law.com

/s/Paul J. Doolittle
Paul J. Doolittle (*Pro Hac Vice* Forthcoming)
POULIN | WILLEY | ANASTOPOULO
32 Ann Street
Charleston, SC 29403
Telephone: (803) 222-2222
Fax: (843) 494-5536
Email: paul.doolittle@poulinwilley.com
cmad@poulinwilley.com

Attorney for Plaintiff and Proposed Class